



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/306,110	05/06/1999	SATOSHI HASEGAWA	P/2850-19	3039

7590 06/22/2005

Dickseim Shapiro Morin & Oshinsky LLP  
1177 Avenue of the Americas  
NEW YORK, NY 10036-2714

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 06/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/306,110

Applicant(s)

HASEGAWA, SATOSHI

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 April 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-9,11 and 14-17 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-9,11 and 14-17 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 October 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Arguments***

1. Applicant's arguments with respect to claims 1,2,4-9,11,14-17 have been considered but are moot in view of the new grounds of rejection.

### ***Drawings***

2. Figure 6 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). According to the applicant's specification, page 2, lines 20-22, it is recited of convention data transmission systems that is a prior art disclosure. Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1,2,5,6,8,9, and 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser in view of Jones.

As per claims 1 and 17, it is disclosed by Wiser of calculation means for performing calculation using a key (variable) on an original data stream read from a recording medium so as to produce a encrypted (calculated) data stream (column 2, lines 25-28); variable creation means for creating the key (variable)(column 4, lines 60-65); a stream buffer (column 2, lines 24-25); decryption (inverse calculation) means for performing decryption (inverse calculation) on the calculated data stream output from the stream buffer to reproduce the data stream (column 2, lines 29-34;); stream processing means (column 2, 55-57); output means (column 2, 31-32). The teachings of Wiser fail to disclose of using a key (variable) to reproduce the data stream and that the key (variable) is changeable at a regular timing. Wiser does teach that any encryption/decryption method may be used in his system (column 8, lines 50-51). It is disclosed by Jones of pseudo-random number generates that uses a seed value and counter (i.e. regular timing) to generate a variable used for encrypting a data stream (column 3, line 60 through column 4, line 12). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a changing key based on regular timing. The teachings of Jones recite of motivation for modifying a key based on a counter in that by changing encryption keys frequently, it reduces the opportunity that an illegitimate user can decrypt the data (column 1, lines 22-24). It is obvious that the teachings of Wiser would have found the teachings of

Jones beneficial in an attempt to further secure the data against an unauthorized user being able to decrypt the data.

As per claim 2, Wiser teaches the data streams is read from the recording medium corresponds to an amount of data which can be processed at a time (column 2, lines 20-21).

As per claim 5, the teachings of Wiser disclose of calculation means for performing encryption (calculation) using a variable on an original data stream read from a recording medium so as to produce a encrypted (calculated) data stream (column 2, lines 25-28); variable creation means; for creating the key (variable)(column 4, lines 60-65); a stream buffer (column 2, lines 24-25); decryption (inverse calculation) means for performing decryption (inverse calculation) on the calculated data stream output from the stream buffer to reproduce the data stream (column 2, lines 29-34); stream processing means (column 2, 55-57); output means (column 2, 31-32). Wiser is silent in disclosing creating a number of variables, one of which is arbitrarily chosen as the key (variable) used for encryption (calculation). Jones discloses of creating a sequence of keys (number of variables), one of which is arbitrarily chosen as the key (variable) used for encryption (calculation)(column 3, line 60 through column 4, line 12). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a changing key based on regular timing. The teachings of Jones recite of motivation for modifying a key based on a counter in that by changing encryption keys frequently, it reduces the opportunity that an illegitimate user can decrypt the data (column 1, lines 22-24). It is obvious that the teachings of Wiser

Art Unit: 2131

would have found the teachings of Jones beneficial in an attempt to further secure the data against an unauthorized user being able to decrypt the data.

As per claim 6, Wiser teaches the data streams is read from the recording medium corresponds to an amount of data which can be processed at a time (column 2, lines 20-21).

As per claim 8, it is disclosed by Wiser of encryption (calculation) means for performing encryption (calculation) using a key (variable) on an original data stream read from a recording medium so as to produce an encrypted (calculated) data stream (column 2, lines 25-28); variable creation means for creating the key (variable)(column 4, lines 60-65); a stream buffer (column 2, lines 24-25); inverse calculation means for performing decryption (inverse calculation) on the encrypted (calculated) data stream output from the stream buffer to reproduce the data stream (column 2, lines 29-34); stream processing means (column 2, 55-57); output means (column 2, 31-32). Wiser is silent in disclosing creating a set of keys (variables) and producing key (variable change codes) representing the key (variable) selected from the key sequence (variable set). Wiser does teach that any encryption/decryption method may be used in his system (column 8, lines 50-51). Jones discloses of creating a sequence of keys (number of variables) used for encryption (calculation) and producing key (variable change codes) representing the key (variable) selected from the key sequence (variable set) (column 3, line 60 through column 4, line 12). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a changing key based on regular timing. The teachings of Jones recite of motivation for modifying a

key based on a counter in that by changing encryption keys frequently, it reduces the opportunity that an illegitimate user can decrypt the data (column 1, lines 22-24). It is obvious that the teachings of Wiser would have found the teachings of Jones beneficial in an attempt to further secure the data against an unauthorized user being able to decrypt the data.

As per claim 9, Wiser is silent in disclosing a changing the variable after each cycle. Wiser does teach that any encryption/decryption method may be used in his system (column 8, lines 50-51). It is disclosed by Jones of pseudo-random number generates that uses a seed value and counter (i.e. end of cycle) to generate a variable used for encrypting a data stream (column 3, line 60 through column 4, line 12). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a changing key based on regular timing. The teachings of Jones recite of motivation for modifying a key based on a counter in that by changing encryption keys frequently, it reduces the opportunity that an illegitimate user can decrypt the data (column 1, lines 22-24). It is obvious that the teachings of Wiser would have found the teachings of Jones beneficial in an attempt to further secure the data against an unauthorized user being able to decrypt the data.

As per claims 15 and 16, Wiser discloses of encryption (calculation) means for performing encryption (calculation) using a key (variable) on an original data stream read from a recording medium so as to produce an encrypted (calculated) data stream (column 2, lines 25-28); variable creation means for creating the variable (column 4, lines 60-65); a stream buffer (column 2, lines 24-25); decryption (inverse calculation)

means for performing inverse calculation on the calculated data stream output from the stream buffer to reproduce the data stream (column 2, lines 29-34); stream processing means (column 2, 55-57); output means (column 2, 31-32). Wiser does teach that any encryption/decryption method may be used in his system (column 8, lines 50-51).

Wiser is silent in disclosing creating a number of keys (variables) and that the keys (variable) change codes periodically. Wiser does teach that any encryption/decryption method may be used in his system (column 8, lines 50-51). It is disclosed by Jones of pseudo-random number generates that uses a seed value and counter (i.e. periodic) to generate a variable used for encrypting a data stream (column 3, line 60 through column 4, line 12). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a changing key based on regular timing. The teachings of Jones recite of motivation for modifying a key based on a counter in that by changing encryption keys frequently, it reduces the opportunity that an illegitimate user can decrypt the data (column 1, lines 22-24). It is obvious that the teachings of Wiser would have found the teachings of Jones beneficial in an attempt to further secure the data against an unauthorized user being able to decrypt the data.

5. Claims 4,7,11, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al in view of Jones, in further view of Mionet et al.

As per claims 4, 7, 11, and 14, the examiner supplies the same rationale as recited in the rejection of claim 1 for the motivation to include the teachings of Jones within the system of Wiser. Wiser and Jones are silent in disclosing a message



Art Unit: 2131


representing a variable change code. Mionet teaches that in order for the decrypting device to know when to use a new key, that the encryption device sends a message to the decrypting device indicating when a new key is to be used (column 9, line 65-column 10, lines 15). Mionet uses a message to indicate a key change instead of just sending the new key over the transmission means. If one were to send the new key encrypted with the old key and the old key had been comprised then the new key would also be compromised. It is inherently insecure to send a key in the clear. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to pass a variable change code from the calculator to the inverse calculator because it is more secure than sending the new key encrypted by the old key. In the context of Wisner, it is obvious that the code must travel from the calculator to the inverse calculator via the buffer because that is the only data path to connecting the two.

### ***Conclusion***

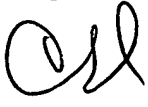
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR  
  
June 15, 2005

Christopher Revak  
AU 2131

  
6/15/05